I**nformation Security Policy**

Category: Governance
Responsible Office: Information Technology & Computing Services
Responsible Administrator: Vice President of Strategy and Innovation
Date Effective: 12/01/2025
Date Last Revised: 11/12/2025
Date Posted to Library: 12/03/2025

POLICY SUMMARY

This policy defines San Francisco Bay University's (SFBU) framework for protecting the confidentiality, integrity, and availability of institutional information and technology resources. It establishes expectations for secure and ethical use in alignment with the *SFBU Employee Handbook* and related policies.

POLICY

Policy Statement

SFBU is committed to protecting its information assets against unauthorized access, disclosure, alteration, or destruction. The University recognizes that its data, technology systems, and digital communications are vital resources that support teaching, learning, research, and administration. Therefore, all information created, stored, or transmitted on SFBU systems is the property of the University and must be used responsibly and securely.

SFBU's Information Security Policy is aligned with the Center for Internet Security (CIS) Controls, NIST Special Publication 800-53 (Moderate Baseline), and regulatory requirements, including FERPA and applicable privacy laws.

Information security is a shared responsibility. Faculty, staff, students, and third-party vendors must adhere to this policy and other related standards. Each member of the SFBU community plays a vital role in maintaining the protection of the University's information.

Applicability

This policy applies to all SFBU employees, students, contractors, vendors, and affiliates who access, store, or process University data through University-owned or University-approved systems, devices, or services. It covers all technology resources owned, leased, or managed by SFBU, as well as third-party systems with University data access.

This policy does not apply to:

- Personally Identifiable Information (PII) data or systems unrelated to the University's academic portfolio or business operations.
- Data explicitly designated for public release.

Procedure

SFBU adopts baseline controls, also referred to as minimum security standards, consistent with operational best practices:

Access Control

- Privileged access shall be managed under “least-privilege principles.” Under the least privilege principle, users are granted only the minimum level of access and permissions necessary to perform their specific work functions.
- Access to University systems is restricted to authorized users. Multi-factor authentication (MFA) must be used for systems containing confidential or restricted data.
- Access privileges will be reviewed annually and revoked promptly when no longer needed.

Data Protection

- Restricted and confidential data must be encrypted, both in storage and during transmission.
- Portable devices and removable media must employ encryption and password protection.
- Storing University data on unapproved personal devices or cloud systems is prohibited.

Generative Artificial Intelligence (AI)

- AI systems must not process PII or regulated data unless anonymized.
- AI tools licensed by SFBU must comply with University information security standards and the Generative AI Policy.
- Data used to train or processed through AI systems must be classified appropriately, and restricted or confidential data may only be used in licensed AI platforms approved by “ITCS”.

System and Network Security
- University systems must use supported software versions, apply security patches in a timely manner, and maintain up-to-date malware protection. In cases where systems cannot be updated due to operational, compatibility, or vendor limitations, such exceptions must be documented, risk-assessed, and approved by IT before continued use.
- Users must not disable security settings or install unauthorized applications.

System and Network Monitoring
- The University may monitor and review network traffic and usage for compliance, safety, and performance.
- Users should not expect privacy when using University hardware or software resources.

User Responsibilities
- Employees must complete annual security training, protect their credentials, and secure devices.
- Students are strongly encouraged to attend the training sessions provided by ITCS.
- Unauthorized sharing of credentials, neglecting updates, or storing restricted data insecurely violates this Information Security policy.

Vendor and Third-Party Management
- Third-party vendors must complete SFBU's Vendor Security Assessment before engagement and maintain compliance thereafter.

Compliance and Oversight
The Information Technology & Computing Services (ITCS) department, under the oversight of the Vice President of Strategy and Innovation, is responsible for implementing, monitoring, and enforcing this policy.

Non-compliance with this policy may result in disciplinary action, including termination of employment, expulsion, or legal proceedings. The University reserves the right to suspend access to protect institutional integrity.

Definitions

Availability
Ensuring timely, reliable access to systems and data

Confidential Data
Information that requires controlled access to protect the University's interests or those of affiliated individuals. Examples include internal communications, non-public financial information, and internal research data not intended for external release.

Encryption
The process of converting data into a secure format to prevent unauthorized access.

Incident
An event that threatens the confidentiality, integrity, or availability of University information.

Integrity
Safeguarding the accuracy and completeness of information and processing methods.

Internal Data
Information intended for use within the University community that is not public but does not require the same level of protection as Confidential or Restricted data. Examples include internal procedures, operational plans, and non-sensitive communications.

Least Privileged
Users, applications, and systems are granted only the minimum level of access, permissions, privileges, or data necessary to perform their authorized tasks.

Personally Identifiable Information (PII)
Any data that can directly or indirectly identify an individual, such as name, address, phone number, email address, student ID, or IP address. PII data is often regulated under privacy laws or University policy.

Public Data
Information approved for unrestricted release without risk of harm to the University.

Restricted Data
Highly sensitive information that, if compromised, could cause substantial harm to individuals or the University. Examples include student records (FERPA), personally identifiable information (PII), protected health information (PHI), and financial account details.

Regulated Data
Information that is protected by federal, state, or international laws or regulations. Examples include FERPA-protected student records, HIPAA-protected health data, and payment information governed by PCI DSS. Handling of such data must comply with applicable regulatory requirements.

User
All individuals authorized to access University systems or data, including faculty, staff, students, contractors, vendors, and affiliates.

Responsibility
The Senior Director of Information Technology & Computing Services conducts regular risk assessments, manages incident response, and ensures compliance with applicable regulations and University standards.

RELATED INFORMATION

Acceptable Use Policy
Data Privacy Policy
Generative Artificial Intelligence Policy
IT Incident Reporting Form
SFBU Employee Handbook

CONTACT INFORMATION

Information Technology & Computing Services
Email: itcs@sfbu.edu

REVISION HISTORY

11/05/2025 - Policy reviewed by the Policy Committee
10/31/2025 - Policy created and transferred to the standard policy template

Next Review Date

October 2026

APPROVAL

11/21/2025 - President
11/14/2025 - University Policy Committee

APPENDICES

None

The SFBU enterprise version of ChatGPT was used in the drafting of this policy to support clarity, consistency, and alignment with institutional standards.